Department of Homeland Security Daily Open Source Infrastructure Report for 24 August 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports two people were seen on surveillance tapes cutting through a fence and climbing atop the storage tank at a liquefied natural gas storage facility in Lynn, Massachusetts, last week, and authorities are calling for a full−scale investigation. (See item 1)
- The Department of Homeland Security has released a Fact Sheet update on the Secure Border Initiative program discussing among other topics the end to the “Catch and Release" of illegal aliens at the Southern border. (See item 14)
- CNN reports twelve passengers were in custody Wednesday, August 23, after a Northwest Airlines flight bound for Mumbai, India, returned to Amsterdam with a fighter jet escort; U.S. air marshals broke their cover to aid with the passenger situation. (See item 16)
- The Associated Press reports a terrorism attack sparking the evacuation of several million people from the Washington, DC−area is enough of a concern that West Virginia is hosting a regional conference on the subject Wednesday and Thursday, August 24. (See item 26)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) −

http://www.esisac.com]

1. *August 23, Associated Press* — **Security breach reported at Lynn LNG facility.** Two people were seen on surveillance tapes cutting through a fence and climbing atop the storage tank at a liquefied natural gas storage facility in Lynn, MA, last week, and while it does not appear to be an act of terrorism, authorities are calling for a full−scale investigation. Authorities were especially displeased with the five−day lag between the August 16 security breach and when KeySpan Corp. reported it to the state on Monday, August 21, said Mike Coelho, of the state Executive Office of Public Safety. U.S. Representative Edward J. Markey (D−MA) called on Governor Mitt Romney's administration to "order a comprehensive review of the perimeter security plans at all such critical infrastructure facilities in the Commonwealth to guarantee a future security breach does not occur." Markey also said the "incident raises serious questions about the adequacy of the perimeter security and surveillance monitoring in place at this facility."
   Source: http://www.boston.com/news/local/massachusetts/articles/2006/08/23/security_breach_reported_at_lynn_lng_facility/

2. *August 22, Associated Press* — **NYC official: Con Ed blackout numbers off.** New York City's top emergency coordinator said Tuesday, August 22, that after the Queens blackout, the city will no longer rely solely on Consolidated Edison for information on the magnitude of a power outage. At a city council committee hearing on the Queens outage, Joseph Bruno, the commissioner of the City's Office of Emergency Management (OEM), said Con Edison never told city officials how extensive the outage was in Queens. He said Con Edison advised the city there were 1,700 customers, or 6,800 people, without power on the sixth day of the blackout −− believed to be the peak day of the weeklong failure. City officials now believe that more than 100,000 plus people were in the dark. OEM has established a new system: As soon as there is an indication from Con Edison that more than 1,000 customers are affected or there is a significant impact, an emergency team −− the Power Outage Response Team −− will be sent to survey the area, Bruno said. The 311 emergency telephone line will also be monitored to see if there is a concentrated number of calls from a particular area.
   Source: http://www.chron.com/disp/story.mpl/ap/fn/4133936.html

3. *August 21, Dow Jones* — **Southern Company unit says small amount of nuclear fuel missing.** Southern Company informed the Nuclear Regulatory Commission that less than 1.5 ounces of spent nuclear fuel remains unaccounted for at its Edwin Hatch nuclear plant near Baxley, GA. While small portions of the material might have been inadvertently shipped to a waste disposal facility, Southern Nuclear believes that the balance remains in the spent fuel pools in areas that are either unobservable by camera or otherwise inaccessible. Future preparations for low−level waste shipments will take into account the possibility of the material's presence in the pools, and any residual amount will be retrieved when the plant is decommissioned, Southern Nuclear said.
   Source: http://www.marketwatch.com/News/Story/Story.aspx?dist=newsfinder&siteid=google&guid=%7BF877E682−37A5−4F93−9A05−9BA7A670A853%7D&keyword=

4. *August 21, Reuters* — **Schwarzenegger signs solar power bill.** California Governor Arnold Schwarzenegger on Monday, August 21, signed into law a bill that aims to make the state one

of the world's biggest producers of solar energy. The bill calls for the installation of one million rooftop solar panels on homes, businesses, farms, schools, and public buildings by 2018. The solar systems would generate 3,000 megawatts of power, making California the third biggest solar producer after Japan and Germany. The new law requires homebuilders to offer solar power to home buyers beginning in 2011 and allows utility customers who install panels to sell excess power back to their utility. The law also extends the solar program to municipally owned utilities.
Source: http://today.reuters.com/news/articlenews.aspx?type=politicsNews&storyID=2006−08−21T183641Z_01_N21135076_RTRUKOC_0_US−ENERGY−CALIFORNIA−SOLAR.xml&WTmodLoc=NewsHome−C3−politicsNews− 3

5. *August 20, Xinhua (China)* — **Northeast India to produce electricity from bamboo.** A bamboo−fuelled power station is to be built in Mizoram to help meet the energy needs of India's northeast, according to Indo−Asian News Service. Bamboo would be harvested and then dried before it is processed for feedstock to produce gas, which would finally get converted to electricity. The Mizoram area annually produces 3.2 million tons of bamboo, which has never been tapped to generate electricity. India, the world's largest producer of bamboo after China, grows about 80 million tons each year.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8knpq%5F%5BimlornmTUgct%3EEvbfel%5Dv

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

6. *August 23, Boston.com* — **Software glitch affects student loan Website.** A software glitch at a federal Department of Education student loan account Website allowed some users to access other people's personal information early this week, The Boston Globe reported Wednesday, August 23. The problem affected people who accessed their accounts between Sunday night and Tuesday morning and tried to use certain parts of the Website. Hudson La Force, senior counselor to the Secretary of Education, told the Globe that a routine software upgrade introduced a bug that mixed up the information for different borrowers. "We think the effect is pretty limited," he said, but he did not know how many people's information was compromised. LaForce said officials believe the people who saw each other's information were trying to do the exact same thing on the Website at the same time. LaForce said the department turned off part of the system believed to be affected after a borrower called to report the problem on

Monday, but later turned off other parts of the system when they were found to be malfunctioning as well. Joe Barrett, of Affiliated Computer Services Inc., a contractor that maintains the software that caused the problem, said no identity theft has occurred.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/08/23/report_software_glitch_affects_student_loan_web_site/

7. *August 23, Journal Register (MI)* — **Stolen laptop holds patient information.** Tens of thousands of William Beaumont Hospital Home Care patients could be at risk of having their personal identification used for illegal purposes after a home care nurse's car and laptop were stolen. The theft occurred in early August when the auto was taken from the parking lot of a senior center in east Detroit. The Beaumont laptop contained the personal information of 28,473 Home Care patients from across the metro Detroit area who have used the service over the past three years prior to August 5. Information including patient names, addresses, birth dates, medical insurance information, Social Security numbers, and personal health information related to their home care services was contained in that laptop. Beaumont sent out letters to affected patients on Monday, August 21, and had disabled the login connection to the woman's laptop the Monday after the incident. Between August 5 and August 7, officials say information was not accessed. "Based on the circumstances of the theft, we believe the risk of identity theft is very low," Chris Hengstebeck, director of Beaumont Security, said.
Source: http://www.theoaklandpress.com/stories/082306/loc_2006082339 .shtml

8. *August 22, Northeast Georgian* — **Local Georgia banks warn customers of e−mail scam.** Officials from Habersham County, GA, financial institutions have issued a warning to their customers who may receive an unsolicited e−mail purportedly from the Federal Deposit Insurance Corporation (FDIC). The scam involves disclosure of personal and financial information. FDIC released an alert on August 15 that said the scam e−mail claims that the FDIC has received an application from the receipt's bank to insure their checking or savings account against fraud, phishing, and identity theft. The e−mail instructs the recipient to enroll in the FDIC protection system by clicking on a link to a spoofed FDIC Web page, and then requests personal information.
Source: http://www.thenortheastgeorgian.com/articles/2006/08/22/news/business/01business.txt

9. *August 22, Kansas City Channel (KS)* — **Feds arrest alleged identity theft ring.** Local Kansas City, KS, and federal authorities made a sweep of arrests Tuesday, August 22, in a large identity theft and fraud ring, officials said. Investigators said the case started with identity theft, but it spread into mortgage fraud, money laundering, and possibly drug trafficking all over the country. Sixteen people were charged in the case, but officials said there are about 50 suspects in the case. Officials said the suspects would take personal credit information and turn it into forged documents and driver's licenses. The indictment claimed the suspects had access to a personal computer that could create a counterfeit Kansas driver's license. It would have name of an identity theft victim, but the picture of one of the conspirators. The suspects would then use the fraudulent documents to buy items on other people's credit, including real estate transactions, all of which drained millions of dollars from the community, officials said. The Kansas City Financial Crimes Task Force led the probe, which is headed by the Secret Service.
Source: http://news.yahoo.com/s/kmbc/20060822/lo_kmbc/9720072

10. *August 22, Websense Security Labs* — **Phishing Alert: Taylor County Bank.** Websense Security Labs has received reports of a new phishing attack that targets customers of Taylor County Bank, which is based in Kentucky. Users receive a spoofed e−mail message claiming that a new security system has been put in place, and it needs to be activated. The link provided in the e−mail leads to a phishing site that attempts to collect users' account information.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=582

11. *August 22, Reuters* — **Banks have work cut out fighting terror finance.** As banks get drawn deeper into efforts to counter terrorism, the skills they have developed to trace drug traffickers and criminals are used increasingly to help authorities catch potential bomb plotters. But despite investing large sums to obstruct drug traffickers from using banks to launder money, lenders still face a big challenge identifying terror networks in their midst. Banks say they are becoming more adept at spotting account holders who receive suspicious cash deposits, which could be the proceeds of crime, and quickly passing on that information to investigators who might then find links with terrorism. But banks say they are still in the dark when it comes to trawling through transactions and spotting patterns that might immediately identify an account holder with potential ties to terrorism. Banks are investing heavily in improved searching and matching software, which allows them quickly to home in on account holders when the authorities present them with lists of terrorism suspects to run checks on. "A key battle we have won is that financial institutions are keeping records that need to be there, and providing them to intelligence institutions when they need them," said Vincent Schmoll, at the Paris−based Financial Action Task Force.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/08/22/AR2006082200619_pf.html

[Return to top]

Transportation and Border Security Sector

12. *August 23, Associated Press* — **Two jets return to Seattle−Tacoma International Airport.** Two jetliners were forced to return to the Seattle−Tacoma airport Tuesday, August 22, after they developed problems shortly after takeoff. Engine trouble forced American Airlines Flight 526 headed for Chicago to turn back and make an emergency landing early Tuesday soon after the compressor in one of the MD−80's two engines stalled. Tuesday afternoon, United Airlines Flight 875 bound for Tokyo also turned around and landed at the airport after the crew reported an odor. Elsewhere Tuesday, American Airlines Flight 1107 −− departing Tampa for Dallas −− immediately returned to the airport when its nose gear doors failed to close. The pilot reported a strange vibration and asked to return to Tampa. Afterward, the MD−80 aircraft was taken out of service for repairs, said Tim Wagner, a spokesperson for Fort Worth−based American.
Source: http://www.boston.com/news/nation/articles/2006/08/23/2_jets_return_to_wash_airport_1156310696/

13. *August 23, Washington Post* — **Pressures on airport workers increase; safety conditions draw scrutiny.** Airport ground workers fix planes and load and unload heavy bags in sweltering heat and frigid cold. They do their jobs amid the deafening roar of aircraft engines and the arrival and departure of tanker−size jetliners. Now the ground workers' tough conditions are coming under closer scrutiny. For the first time, airlines and the Federal Aviation

Administration will co−host a three−day symposium focused on improving safety on the tarmac at the nation's airports. Participants in the gathering, which begins September 6, will analyze data on accidents to help airlines identify dangers and adopt strategies for reducing risks. While serious injuries and death do occur, the most common injuries among ground workers result from heavy lifting, in many cases causing severe back strain. So far this year, however, four ground workers have been killed or seriously injured, according to data collected by the Washington Post. Through the busy summer season, ground workers have been under increased pressure to load and unload bags swiftly and to ensure that the aircraft are prepared for safe travel. Many financially strapped carriers have reduced their staffs, leaving more work for the remaining employees.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/08/22/AR2006082200968.html

14. *August 23, Department of Homeland Security* — **Fact Sheet: Secure Border Initiative update.** The Department of Homeland Security has released a Fact Sheet on the Secure Border Initiative program. Among other topics covered, the Fact Sheet states the end to “Catch and Release." In the week of August 7−13, 2006, U.S. Customs and Border Protection apprehended 1055 non−Mexican illegal aliens at the Southern border, and released only seven non−Mexican illegal aliens. And, in conjunction with federal, state, and local partners, and as part of the broader border security and interior enforcement strategy, the Department of Homeland Security has launched targeted border enforcement operations to target violent street gangs and other criminal elements within U.S. communities.
Source: http://www.dhs.gov/dhspublic/display?content=5808

15. *August 23, Associated Press* — **Massachusetts airport left without commercial airline.** Worcester Regional Airport's only commercial airline has told city officials it will cease operations September 3. Allegiant Air said the rising cost of fuel is forcing an end to the economy airline's nine−month stint ferrying passengers between Worcester, MA, and Orlando−Sanford International Airport in Florida, despite 85 to 90 percent capacity. Allegiant becomes the 13th commercial carrier to come and go since 1988, when five commercial airlines served the Worcester airport. Worcester Regional Airport is being managed by the Massachusetts Port Authority until June 2007.
Worcester Regional Airport Website: http://www.massport.com/worce/
Source: http://www.turnto10.com/travelgetaways/9724068/detail.html

16. *August 23, CNN* — **Northwest jet turns back; 12 arrested.** Twelve passengers were in custody Wednesday, August 23, after a Northwest Airlines flight bound for Mumbai, India, returned to Amsterdam with a fighter jet escort, Dutch police said. An airport policeman said authorities have enough information to hold the 12 for at least three days. Flight 42, which originated in Northwest's main hub of Minneapolis−St. Paul International Airport, returned to Amsterdam's Schiphol Airport "after several passengers displayed behavior of concern," Northwest Airlines said in a written statement. Some of the 12 passengers pulled out cell phones during the flight and appeared to be trying to pass the cell phones to other passengers, a U.S. government official said. In addition, some passengers unfastened their seatbelts while the light requiring they be fastened was still illuminated, the official said. That was enough for U.S. air marshals aboard the DC−10 to break their cover. In general, federal air marshals do not identify themselves to passengers if they believe the crew can handle a situation without

assistance. The passengers who were arrested were looking into plastic bags and were busy with their cell phones, an airline source in Amsterdam said.
Source: http://www.cnn.com/2006/WORLD/europe/08/23/schiphol/index.ht ml

17. *August 22, Shanghai Daily (China)* — **Love tiff bomb note makes jet turn back.** Airport police in Guangzhou, China, have detained a Hong Kong man with an Australian passport for falsely reporting there was a bomb on a plane bound for Australia, delaying the flight more than seven hours. The China Southern Airlines flight took off on Monday, August 21, from Guangzhou, capital of south China's Guangdong Province. But after flying about 40 minutes, a male passenger told a flight attendant he had discovered a note in the washroom that said the plane would explode, Xinhua news agency reported. After contacting the ground staff, the flight crew decided to turn the plane around. The aircraft touched down at Baiyun International Airport where the 214 passengers were evacuated and went through security checks, and airport police rechecked the luggage and cargo that was aboard the flight. Police later identified the suspect as Huang Zhonghua, 30, a Hong Kong native who is now an Australian citizen. Police said Huang was angry over a failed love affair.
Source: http://www.shanghaidaily.com/art/2006/08/23/289901/Love_tiff _bomb_note_makes_jet_turn_back.htm

18. *August 22, Associated Press* — **Delta bids some regional flights.** Delta Air Lines Inc. said Tuesday, August 22, that it has requested bids for some of its regional jet service, much of which is now handled by its subsidiary Comair. Delta's announcement came a day before Comair was to return to negotiations with its flight attendants. Comair and Delta are trying to emerge from Chapter 11 bankruptcy filed last year, and Comair says it must have concessions from flight attendants to get out of bankruptcy. Atlanta−based Delta said it has requested proposals from Comair and other regional airlines for operating up to 143 of its regional jets, including up to 43 70−seat jets and as many as 50 50−seat jets. Delta said that its request will not change the destinations served. Comair, based across the river from Cincinnati in Erlanger, KY, now has 27 of the 70−seat planes and some of the 50−seat planes. Chautauqua Airlines, Shuttle America, and Freedom Airlines operate some of the regional jet service for Delta, which also is seeking bids for the operation of 50 new 76−seat jets not yet in service. Delta's executive vice president of operations, Joe Kolshak, said the airline is requesting proposals because it needs to cut costs as it restructures.
Source: http://biz.yahoo.com/ap/060822/delta_comair.html?.v=2

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

19. *August 22, U.S. Department of Agriculture* — **Funds for potato cyst nematode survey announced.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns announced

Tuesday, August 22, the availability of nearly $13 million in emergency funding for potato cyst nematode (PCN) survey efforts. The USDA's Animal and Plant Health Inspection Service (APHIS) and the Idaho State Department of Agriculture (ISDA) originally discovered PCN April 19 as part of the Cooperative Agricultural Pest Survey (CAPS), a surveillance program managed jointly by USDA's Animal and Plant Health Inspection Service and state departments of agriculture. USDA will provide approximately seven million dollars to Idaho for surveys and approximately six million dollars will be used for a nationwide PCN survey. PCN is a major pest of potato crops in cool−temperate areas. It primarily affects plants within the potato family including tomatoes, eggplants and some weeds. Affected potato plants may exhibit yellowing, wilting or death of foliage. If left unmanaged, nematodes can cause significant yield loss.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/08/0312.xml

20. *August 22, Animal and Plant Health Inspection Service* — **Oral rabies vaccine distributed in four states.** Wildlife Services, a program within the U.S. Department of Agriculture's Animal and Plant Health Inspection Service will distribute oral rabies vaccine baits in cooperation with the Ontario Ministry of Natural Resources and Cornell University beginning on or about August 22, to prevent the spread of raccoon rabies in portions of Maine, New Hampshire, New York and Vermont. Baits containing oral rabies vaccine will be distributed over rural areas using low−flying twin−engine aircraft and hand baiting will occur in populated regions using ground vehicles. The projected two−week aerial portion of the program will target raccoons and result in the distribution of more than 1.2 million baits covering roughly 9,675 total square miles in four states. The vaccination zone has been established to prevent the northward movement of the raccoon variant of rabies into Canada.
Source: http://www.aphis.usda.gov/newsroom/content/2006/08/rabine06. shtml

[Return to top]

Food Sector

21. *August 23, Reuters* — **China rejects U.S. milk powder.** China has sent back 100 metric tons of powdered milk made in the U.S. because it contained excess levels of nitrite. The powder, which was imported between July 10 and August 10 by a Chinese company, was worth $200,000 and contained almost twice as many nitrates as Chinese law permits.
Source: http://today.reuters.com/news/articlenews.aspx?type=healthNews&storyID=2006−08−23T060701Z_01_PEK282605_RTRUKOC_0_US−CHINA−USA.xml&archived=False

22. *August 23, Reuters* — **Indian activists plan Coca−Cola, Pepsi blockades.** An Indian environmental group said on Wednesday, August 23, it would temporarily paralyze the supply of Coca−Cola and Pepsi products in the country after another group said it had found dangerous levels of pesticides in their drinks. The New Delhi−based Research Foundation for Science, Technology and Ecology said it would blockade trucks of the two beverage companies for five days starting on November 21 as part of its "Quit India" campaign targeting the beverage manufacturers. Both companies maintain their drinks are safe. Experts said the controversy had overshadowed the real issue as pesticide usage in India was high and most farm products were contaminated.

Source: http://www.alertnet.org/thenews/newsdesk/DEL265692.htm

[Return to top]

Water Sector

23. *August 21, Canadian Press* — **City of Montreal closes two−thirds of outdoor pools for failing tests.** A cocktail of bacteria, parasites and viruses in the water of Montreal, Canada's swimming pools has forced the city to close two−thirds of its outdoor facilities. Mayor Gerald Tremblay asked mayors of the city's 19 boroughs to close 48 of the city's 73 outdoor pools following a media investigation. Tests found high levels of E. coli, C. difficile, Legionella, Hepatitis A, and Giardia. The pool closings were ordered following an investigation by tabloid Le Journal de Montreal and the TVA television network. One−third of the pools failed tests conducted by a private firm hired by the media outlets. Another third of the pools had samples that failed to meet accepted standards. Three samples were taken from each pool between July 8 and August 1. In all, some 4,560 samples were evaluated.
Source: http://www.cbc.ca/cp/health/060821/x082120.html

[Return to top]

Public Health Sector

24. *August 23, Associated Press* — **U.S. Centers for Disease Control and Prevention releasing gene blueprints for 650 viruses.** U.S. health officials have placed the genetic blueprints of more than 650 flu viruses into a public database, in an attempt to increase flu research and set an example for other nations. The U.S. Centers for Disease Control and Prevention (CDC) deposited the information last week, CDC officials said Tuesday, August 22. The genetic information is only for naturally circulating viruses isolated in the U.S. It includes data from the annual U.S. flu season, animal flu viruses that infect humans, and new strains that may emerge in the U.S., such as the H5N1 bird flu. The data were deposited in Genbank, a public−access library for virus sequences managed by the National Institutes of Health, and in a database housed at Los Alamos National Laboratories.
Source: http://www.cbsnews.com/stories/2006/08/23/ap/health/mainD8JL U8OG1.shtml

25. *August 22, Agence France−Presse* — **No sign of human bird flu transmission in Indonesia.** Experts have failed to uncover evidence of bird flu spreading between humans in a remote area in Indonesia where three people have been infected with the virus, the World Health Organization (WHO) has said. The WHO experts along with their Indonesian counterparts have been investigating an outbreak of the H5N1 strain in Cikelet, a group of villages in the Garut district of West Java. Three infections have been confirmed −− two of which were fatal −− while three further suspected deaths have occurred since last month, raising fears of a possible bird flu "cluster" case. Such cases, where human−to−human transmission occurs, raise the likelihood of H5N1 mutating into a form easily passed between humans.
Source: http://news.yahoo.com/s/afp/20060822/hl_afp/healthfluindones ia_060822114716

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

26. *August 23, Associated Press* — **Evacuation plan raises concern in West Virginia.** A terrorism attack sparking the evacuation of several million people from the Washington, DC−area is enough of a concern that West Virginia is hosting a regional conference on the subject Wednesday and Thursday, August 24. The state Department of Military Affairs and Public Safety hopes the Urban−Rural Evacuation Conference lays the groundwork for a regional plan for dealing with a mass invasion. About 100 public safety officials from West Virginia, Delaware, Kentucky, Ohio, Pennsylvania, Maryland, Virginia, the District of Columbia, and federal agencies are expected to attend. The focus of the conference, however, won't be on terror risks, but on such topics as how to establish a way for states to talk to each other and pool resources amid a crisis.
Source: http://www.wvgazettemail.com/section/News/2006082227

27. *August 23, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: At 5:00 a.m. EDT Wednesday, August 23, Tropical Storm Debby (formerly Tropical Depression Four) was located near 15.9 north 30.1 west or about 385 miles west−northwest of the Cape Verde Islands with sustained wind speeds near 45 mph. Debby is moving toward the west−northwest near 16 mph and this general motion is expected to continue for the next 24 hours. Eastern Pacific: At 12:00 a.m. EDT Wednesday, Hurricane Ileana with winds about 86 mph was located at 16.6 north 109.2 west southwest of Acapulco, Mexico. Ileana is expected to intensify during the next few days before weakening when it moves into cooler waters. At 5:00 a.m. EDT Wednesday, Hurricane 01C Ioke was located near 17.2 north 170.5 west or about 75 miles WNW of Johnston Island and about 870 miles WSW of Honolulu, HI. The storm, with sustained winds about 105 mph, is moving across open waters and does not currently threaten any U.S. interests.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat082306.shtm

28. *August 22, Network World* — **Alaska's wireless net built for emergency.** Alaska is benefiting from a new $120 million wireless network for emergency communications that was built through a one−of−a−kind partnership between federal, state and local government agencies. The Alaska Land Mobile Radio (ALMR) system took a decade to build because of a lengthy design and approval process for its special spectrum−sharing system. Using emerging IP−based standards, Alaska has built a common communications infrastructure that is being used by federal agencies including the Department of Defense, all state agencies and local police and fire departments. What's unusual about ALMR is that federal and state officials are sharing the cost as well as contributing spectrum. Federal agencies donated spectrum for mobile applications of the system, while the state of Alaska donated spectrum for fixed

communications services. Federal agencies are chipping in 85 percent of the cost of ALMR. The remaining cost is being carried by state and local agencies. Today, ALMR has 9,000 users, but it can support as many as 14,000 users. The P25−compliant system offers integrated voice and data. Each radio site is connected via microwave and fiber. Subscribers can use the system for mobile voice and data communications.
Source: http://www.networkworld.com/news/2006/082806−wireless−alaska .html

29. *August 20, Associated Press* — **Kansas first responders receive chemical response training from transportation industry.** Emergency crews throughout Kansas are getting special training from the transportation industry on responding to chemical spills, fires and other mishaps involving trains and trucks. A group called TransCAER −− Transportation Community Awareness and Emergency Response −− is holding regional disaster training sessions in 10 Kansas communities this month and next. “We’re learning about the construction of the trucks, how the rail cars operate, and it’s really valuable information we need to help protect the public,” said Capt. Brian Hoy of the Wichita Fire Department. Hoy and colleagues from as far away as Parsons learned Friday, August 18, where to find and how to operate shut−off valves and pressure valves, and where to most likely find leaks at an accident scene. Actually operating the shut−off valves and seeing the equipment before an emergency gives those who respond familiarity before a crisis.
Source: http://www2.ljworld.com/news/2006/aug/20/chemical_spills_ethanol_fires_focus_disaster_train/?state_regional

[Return to top]

Information Technology and Telecommunications Sector

30. *August 23, BBC* — **Mass e−mail attacker pleads guilty.** David Lennon, 19, who bombarded the UK's Domestic & General Group with 5 million e−mails, causing its server to collapse, was sentenced on Wednesday, August 23, to a two−month curfew after pleading guilty. Lennon was a part−time employee of the company before he was fired in 2003.
Source: http://news.bbc.co.uk/1/hi/uk/5278772.stm

31. *August 23, Sophos* — **PC users stung by credit card chargeback Trojan horse.** Sophos has warned of a Trojan horse that has been spammed out claiming that the recipient's credit card has been charged. Sophos has received reports of the Troj/Dloadr−AMA Trojan horse, which arrives in a message claiming to come from a company called Cihost, at e−mail gateways across Europe. The malicious e−mails have the subject line, "[paycheck 322082] Credit Card Chargeback." Attached to the e−mails is a file called PAYCHECK.ZIP, unpacks to paycheck_322082.exe. Executing this file infects the user's computer with a Trojan horse that attempts to download further malicious code from the Internet.
Source: http://www.sophos.com/pressoffice/news/articles/2006/08/credit−card−chargeback.html

32. *August 22, Security Focus* — **Microsoft Office routing slip processing remote buffer overflow vulnerability.** Microsoft Office is prone to a remote buffer−overflow vulnerability. Analysis: This vulnerability occurs when the application handles a specially crafted document.

A successful attack can result in a remote compromise in the context of an affected user. This issue is known to be exploited in the wild by malware. In particular, "Trojan.PPDropper" is known to exploit this issue.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/17000/info
Solution: Microsoft has released fixes to address this vulnerability in supported versions of the affected software. Avaya has released advisory ASA−2006−069 to identify vulnerable Avaya products. Avaya advises customers to apply patches released by Microsoft. Please see references for more information: http://www.securityfocus.com/bid/17000/references
Source: http://www.securityfocus.com/bid/17000/discuss

33. *August 22, eWeek* — **IE patch introduces new exploitable vulnerability.** On the same day Microsoft was expected to re−release an Internet Explorer (IE) security update, a private security research outfit warned that the original patch actually introduced an exploitable vulnerability. The new warning comes less than a week after Microsoft offered a private hotfix for the browser because of a glitch that caused unexpected crashes. However, according to an advisory from eEye Digital Security, the browser crash could cause a "high risk" buffer overflow that could lead to code execution attacks. Microsoft confirmed eEye's new discovery and said the updated IE patch would be delayed indefinitely. Microsoft also posted a security advisory that pinpointed the issue as "long URLs to sites using HTTP 1.1 and compression."
Microsoft Security Advisory: http://www.microsoft.com/technet/security/advisory/923762.mspx
Source: http://www.eweek.com/article2/0,1895,2007109,00.asp

34. *August 22, CNET News* — **Worm sparks rise in zombie PCs.** Malicious code that exploits a recent Windows hole has led to significant growth in the number of hijacked PCs, according to messaging security company CipherTrust. On Tuesday, August 22, CipherTrust reported a 23 percent growth in the total number of so−called zombie PCs it has detected. The jump is due to the spread of Mocbot worm variants, CipherTrust said. Mocbot, also known as Cuebot and Graweg, exploits a Windows security flaw for which Microsoft issued a patch with security bulletin MS06−040 on August 8.
Source: http://news.com.com/Worm+sparks+rise+in+zombie+PCs/2100−7349_3−6108409.html?tag=cd.top

35. *August 22, Tech Web* — **Worm adds MS06−040 to four−bug attack kit.** A network−aware worm that's added the MS06−040 vulnerability to its bag of exploitable bugs is on the make, Symantec said Tuesday, August 22. Dubbed "Randex.gel," the worm opens a back door on any compromised computer, then tells the system to listen for additional commands over an Internet Relay Chat channel. "It looks like it's a derivative of other Randex variants," said Oliver Friedrichs, director of Symantec's security response group. Earlier variations of the Randex worm clan exploited other patched flaws in Windows, including three fixed by MS04−007, MS05−017, and MS05−039. Randex.gel adds the vulnerability in the Windows Server service that Microsoft patched August 8 to the three−some. The new Randex variant can spread in several different ways, Symantec's analysis reported, including via the MSN Messenger, AOL Instant Messenger, Yahoo Messenger, and ICQ instant messaging clients. It will also propagate through network shares and Microsoft SQL servers. In addition, the worm tries to steal account information when users of the eGold electronic payment system log onto the egold.com Website.

Source: http://www.techweb.com/wire/security/192203094;jsessionid=OK5Z524N33FC4QSNDLPCKH0CJUNN2JVN

36. *August 22, IDG News Service* — **U.S. Government lab offers open−source grid computing toolkit.** A new open−source software toolkit became available Tuesday, August 22, to improve remote online scientific collaboration via grid computing. The Access Grid Toolkit from the U.S. Department of Energy's Argonne National Laboratory enables development of programs to share video, audio, data and text for real−time collaboration between people at different locations around the world. This is the third version of the toolkit, supporting wall−sized display technology, detailed visualization of simulations, a streamlined user interface and other improvements. Since first being offered, the toolkit has been downloaded more than 20,000 times in 56 countries. Access Grid is written in the Python programming language and features more "robust middleware" than the previous version, making it easier for software developers to write applications to run on Access Grid, said Thomas Uram, technical lead for the Access Grid effort with the Futures Laboratory at Argonne. The increased bandwidth afforded by grid computing and the improved interactive features of the software enhance the collaborative environment even when collaborators are miles, or even oceans apart.
Source: http://www.infoworld.com/article/06/08/22/HNgovtgridtoolkit_1.html

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4672 (eMule), 54856 (−−−), 445 (microsoft−ds), 139 (netbios−ssn), 113 (auth), 80 (www), 25 (smtp), 32794 (−−−), 135 (epmap) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

37. *August 23, KFMB (CA)* — **Cameras to be installed at two California schools.** Surveillance cameras are going to be installed on a pair of school campuses in the Oceanside school district. The district board voted unanimously Tuesday night, August 22, to put cameras at both Oceanside High School and Laurel Elementary School. Both schools have recently undergone renovations, and the cameras are intended to help protect that investment, along with keeping kids safe. The two schools have been hit hard by vandals in the past, especially at Laurel Elementary, where vandals caused an estimated $20,000 in damages.
Source: http://www.kfmb.com/story.php?id=60893

38. *August 23, Daily News Record (VA)* — **Virginia's Spotswood High School gets video cameras.** Spotswood High School will soon be under video surveillance, officials say. According to Rockingham County, VA, Schools Superintendent John Kidd, video cameras are

being installed in the school's hallways and on its grounds, making Spotswood the first school in the county to have surveillance cameras. Kidd said the cameras are being installed at the school to help curb vandalism and provide protection to the building, which is isolated from passersby. "We've had more vandalism there than anywhere else" in the county, Kidd said. The cameras will give security to the school that "sets in a location that's off the main road." Spotswood Principal Tim Woodward said six or seven cameras are being installed in strategic locations around the building and at "main travel areas" within the school. He said the cameras, paid for with donated funds, are a preventative measure. The cameras will add to the school's safety, Woodward said, by helping administrators supervise busy hallways that are often difficult to monitor and by guarding the exterior of the building.
Source: http://www.rocktownweekly.com/news_details.php?AID=5941&CHID =2

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer